What is claimed is:

1. A method for maintaining computer security comprising:

providing a signature file;

receiving an incoming message from at least one client computer;

comparing the received incoming message with the signature file to determine whether the incoming message is malicious; and

blocking the incoming messages determined to be malicious from reaching a web server.

2. The method of claim 1, wherein the comparing further comprises:

parsing the incoming message;

converting the incoming message into an internal format;

comparing the converted incoming message with the signature file; and

determining whether the converted incoming message is malicious based on the comparison.

3. The method of claim 2, further comprising reassembling the converted incoming message back into its original format prior to forwarding it to the web server if it is determined that the code is not malicious.

4. The method of claim 3, further comprising forwarding the reassembled message to the web server.

5. The method of claim 1, wherein the signature file contains information about known system vulnerabilities.

6. The method as claimed in claim 1, wherein the signature file is made available through a web server.

7. The method as claimed in claim 1, further comprising continuously updating the signature file.

8. The method as claimed in claim 1, further comprising periodically downloading the signature file in order to make its copy current.

9. A system for maintaining computer security comprising:

a signature file;

a web server; and

a proxy machine receiving an incoming message from at least one client computer,

comparing the received incoming message with the signature file to determine whether the incoming message is malicious and blocking incoming messages determined to be malicious from reaching the web server.

10. The system of claim 9, wherein the proxy machine further comprises:

an HTTP message parser module for receiving, parsing and converting the incoming messages into a defined format;

an HTTP message analyzer module for comparing the converted incoming messages with the signature file; and

an HTTP message reassembly module for reassembling the converted incoming messages determined not to be malicious into their original format and forwarding them to the web server.

11. The system of claim 9, wherein the signature file contains information about known system vulnerabilities.

12. The system of claim 9, wherein the signature file is made available through a web server.

13. The system of claim 9, wherein the signature file is continuously updated.

14. The system of claim 9, wherein the proxy machine periodically downloads the signature file in order to make its copy current.

15. The system of claim 10, wherein the signature file is linked to the HTTP message analyzer module.

16. A computer storage medium including computer executable code for maintaining computer security, comprising:

code for accessing a signature file;

code for receiving an incoming message from at least one client computer;

code for comparing the received incoming message with the signature file to determine whether the incoming message is malicious; and

code for blocking the incoming messages determined to be malicious from reaching a web server.

17. The computer recording medium of claim 16, further comprising:

code for parsing the incoming message;

code for converting the incoming message into an internal format;

code for comparing the converted incoming message with the signature file; and

code for determining whether the converted incoming message is malicious based on the comparison.

18. The computer recording medium of claim 17, further comprising code for reassembling the converted incoming message back into its original format if it is determined that the code is not malicious.

19. The computer recording medium of claim 18, further comprising code for forwarding the reassembled message to the web server.

20. The computer recording medium of claim 16, wherein the signature file contains information about known system vulnerabilities.

21. The computer recording medium of claim 16, wherein the signature file is made available through a web server.

22. The computer recording medium of claim 16, further comprising code for continuously updating the signature file.

23. The computer recording medium of claim 16, further comprising code for periodically downloading the signature file in order to make its copy current.

24. The method of claim 1, wherein the incoming message comprises an HTTP messages.

25. The system of claim 9, wherein the incoming message comprises an HTTP messages.

26. The computer storage medium of claim 16, wherein the incoming message comprises an HTTP message.